**IN THE UNITED STATES DISTRICT COURT**
**FOR THE NORTHERN DISTRICT OF GEORGIA**

| | |
|---|---|
| KENNETH HASSON and CHAD GRADDY, individually and on behalf of all others similarly situated,<br><br>Plaintiffs,<br><br>v.<br><br>AT&T MOBILITY LLC and AT&T, INC.,<br><br>Defendants. | Case No.: _____<br><br>**CLASS ACTION COMPLAINT**<br><br>**DEMAND FOR JURY TRIAL** |

## CLASS ACTION COMPLAINT

Plaintiffs Kenneth Hasson and Chad Graddy (collectively "Plaintiffs"), by and through their undersigned counsel, file this Class Action Complaint individually and on behalf a class of all similarly situated persons against Defendants and AT&T Mobility LLC and AT&T, Inc. (collectively, "AT&T" or "Defendants"). Plaintiffs base the following allegations upon information and belief, investigation of counsel, and their own personal knowledge.

## NATURE OF THE ACTION

1. Plaintiffs bring this action against AT&T for its failure to properly secure and safeguard highly valuable, protected, personally identifiable information including, *inter alia*, current and former customers' full names, email addresses, phone numbers, dates of birth, AT&T account numbers, Social Security Numbers,

and AT&T account passcodes (collectively, "PII"), failure to comply with industry standards to protect information systems that contain PII, and failure to provide adequate notice to Plaintiffs and other members of the Class that their PII had been accessed and compromised.

2. AT&T is one of the largest companies in the telecommunications sector, and provides internet services and products, cable television, a mobile 5G network, and landline telephone services and products to individuals and businesses across the United States.

3. In order to obtain AT&T's services, customers are required to entrust AT&T with their PII, which AT&T uses in order to perform its regular business activities.

4. Nearly three years ago in 2021, a threat actor claimed to be selling the stolen personal information of approximately 73 million AT&T customers. At the time, AT&T denied that it suffered a data breach or that the data originated from AT&T.[1]

5. Fast forward to March 2024, threat actors began releasing the stolen personal information on the Dark Web, claiming that it was the same dataset

[1] Lawrence Abrams, *AT&T confirms data for 72 million customers leaked on hacker forum*, BleepingComputer (Mar. 30, 2024), https://www.bleepingcomputer.com/news/security/atandt-confirms-data-for-73-million-customers-leaked-on-hacker-forum/#google_vignette.

previously advertised for sale in 2021.[2] However, after previously denying that the data belonged to AT&T customers, on March 30, 2024, Defendants confirmed that the data released on the dark web was that of AT&T customers.[3] The information included 7.6 million current and 64.4 million former customers' full names, email addresses, phone numbers, dates of birth, AT&T account numbers, Social Security Numbers, and AT&T account passcodes (the "Data Breach").[4]

6. As a direct and proximate result of AT&T's failure to implement and follow basic security procedures to protect the PII that it was entrusted and to timely notify its customers of a data breach impacting their PII, Plaintiffs' and Class Members' PII is now in the hands of cybercriminals, has been offered for sale on the dark web, and has been leaked on the dark web.

7. Plaintiffs and Class Members are now at a significantly increased and certainly impending risk of fraud, identity theft, and other harms caused by the unauthorized disclosure of their PII—risks which may last for the rest of their lives. Consequently, Plaintiffs and Class Members must devote substantially more time, money, and energy to protect themselves, to the extent possible, from these crimes.

---

[2] *Id.*

[3] *AT&T Addresses Recent Data Set Released on the Dark Web*, AT&T (Mar. 30, 2024), https://about.att.com/story/2024/addressing-data-set-released-on-dark-web.html.

[4] Khristopher J. Brooks, *What customers should know about AT&T's massive data breach*, CBS News (Apr. 2, 2024), https://www.cbsnews.com/news/att-data-breach-2024-cbs-news-explains/.

8. As such, on behalf of themselves and all others similarly situated, Plaintiffs bring claims for negligence, negligence *per se*, breach of implied contract, unjust enrichment, and declaratory judgment, seeking damages and injunctive relief.

## PARTIES

9. Plaintiff Kenneth Hasson is an adult who at all relevant times is a resident and citizen of the Commonwealth of Pennsylvania and whose PII was compromised by AT&T.

10. Plaintiff Chad Graddy is an adult who at all relevant times is a resident and citizen of the State of Tennessee and whose PII was compromised by AT&T.

11. Defendant AT&T Mobility LLC is a Delaware limited liability company with its principal place of business at 1025 Lenox Park Blvd., NE, Atlanta, GA 30319. AT&T Mobility's ultimate parent company is AT&T Inc. Upon information and belief, AT&T Mobility LLC has four members: BellSouth Mobile Data, Inc.; SBC Long Distance, LLC; AT&T Investment & Tower Holdings, LLC; and New Cingular Wireless Services, Inc.

12. BellSouth Mobile Data, Inc. is a Georgia corporation with a principal place of business at 1025 Lenox Park Blvd., NE, Atlanta, GA 30319.

13. SBC Long Distance, LLC is a Delaware limited liability company. SBC Long Distance, LLC has one member: SBC Telecom, Inc, which is a Delaware corporation with a principal place of business at 208 S. Akard St., Dallas, TX 75202.

14. AT&T Investment & Tower Holdings, LLC is a Delaware limited liability company with four members: AT&T Capital Services, Inc.; SBC Portfolio Holdings, LTD.; SBC Telecom, Inc.; and JVI General Partnership. AT&T Capital Services, Inc. is a Delaware corporation with a principal place of business at 36 S. Fairview Ave, First Floor, Park Ridge, IL 60068. SBC Portfolio Holdings, LTD. is a Delaware corporation with a principal place of business at 208 S. Akard St., Dallas, TX 75202. JVI General Partnership is a Delaware partnership with two partners: AT&T Corp. and AT&T Solutions, Inc. AT&T Corp. is a New York corporation with a principal place of business located at One AT&T Way, Bedminster, NJ 07921. AT&T Solutions, Inc. is a Delaware corporation with a principal place of business located at 15 Vreeland Road, Florham Park, NJ 07932. AT&T Mobility is a citizen of the states of each of its members.

15. New Cingular Wireless Services, Inc. is a Delaware corporation with a principal place of business at 1025 Lenox Park Blvd., NE, Atlanta, GA 30319.

16. AT&T Mobility LLC is therefore a citizen of Delaware, Georgia, Illinois, New Jersey, New York, and Texas.

17. Defendant AT&T, Inc. is a Delaware limited liability company that maintains its headquarters at 208 South Akard Street, Dallas, TX 75201. AT&T, Inc. is a citizen of the state in which it is incorporated and in which it is headquartered and is therefore a citizen of Delaware and Texas.

18. To the extent that the true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, including the named members of the Defendant LLC who are only known to Defendants and who may be responsible for some of the claims alleged herein, are currently unknown to Plaintiffs, Plaintiffs will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known, including any other members of the LLC.

## JURISDICTION AND VENUE

19. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d), the Class Action Fairness Act, because Plaintiffs and at least one member of the Class, as defined below, are citizens of a different state than Defendants, there are more than 100 members of each of the Class, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interests and costs.

20. This Court has personal jurisdiction over Defendants because AT&T has committed acts within the Northern District of Georgia giving rise to this action and has established minimum contacts with this District such that the exercise of

jurisdiction over Defendants would not offend traditional notions of fair play and substantial justice. AT&T has engaged in continuous, systematic, and substantial activities within Georgia, including substantial marking and sales of services and products in connection with the Data Breach within Georgia.

21. This Court is the proper venue for this action pursuant to 28 U.S.C. § 1391(b)(1), because Defendants reside in this District, a substantial part of the events and omissions giving rise to Plaintiffs' claims occurred in this District, Defendants conduct substantial business within this District, and Defendants harmed Class Members residing in this District.

## FACTUAL BACKGROUND

### A. AT&T Provides Telecommunications Services Involving Highly Sensitive PII.

22. AT&T is a leading provider of telecommunications and internet connectivity services in the United States to residential and business customers.[5] AT&T is one of the largest telecommunications companies in the country, with approximately 241.5 million wireless subscribers as of yearend 2023.[6]

[5] *AT&T Business*, AT&T, https://www.business.att.com/?bref=IBBz250012babsbzL (last accessed Apr. 10, 2024).

[6] *AT&T Form 8-K* (Jan. 24, 2024), https://investors.att.com/~/media/Files/A/ATT-IR-V2/financial-reports/quarterly-earnings/2023/4q-2023/ATT_4Q_2023_8_K_Earnings_8_01.pdf.

23. AT&T provides "America's most reliable 5G network."[7] Through its wireless network, AT&T offers "faster data," "lower latency," and can help save energy and enable virtual reality and autonomous cars.[8]

24. In addition to its wireless services, it also offers both business and residential internet services.[9] AT&T claims to offer a 100% fiber network and equal upload and download speeds, something it claims its competitors don't do.[10]

25. In conjunction with providing its telecommunications services, AT&T requires its customers to provide Defendants with their PII, including their full names, email addresses, phone numbers, dates of birth, and Social Security Numbers.

26. In return, Plaintiffs and Class Members reasonably expect that telecommunications providers such as AT&T will use the utmost care to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

27. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' PII, AT&T assumed legal and equitable duties and knew or

---

[7] *Explore AT&T Wireless*, AT&T, https://www.att.com/wireless/ (last accessed Apr. 10, 2024).
[8] *What is 5G?*, AT&T, https://www.att.com/wireless/what-is-5g/ (last accessed Apr. 10, 2024).
[9] *AT&T Business*, *supra* note 5.
[10] *AT&T fiber*, AT&T, https://www.att.com/internet/fiber/ (last accessed Apr. 10, 2024).

should have known that it was responsible for protecting Plaintiffs' and Class Members' PII from disclosure.

28. AT&T itself recognizes that safeguarding its customers information is a "top priority," stating that: "AT&T operates one of the world's most advanced and powerful global backbone networks and is a recognized leading provider of IP-based communication services. We have a responsibility to safeguard customer information. Security is at the core of our network and central to everything we do."[11]

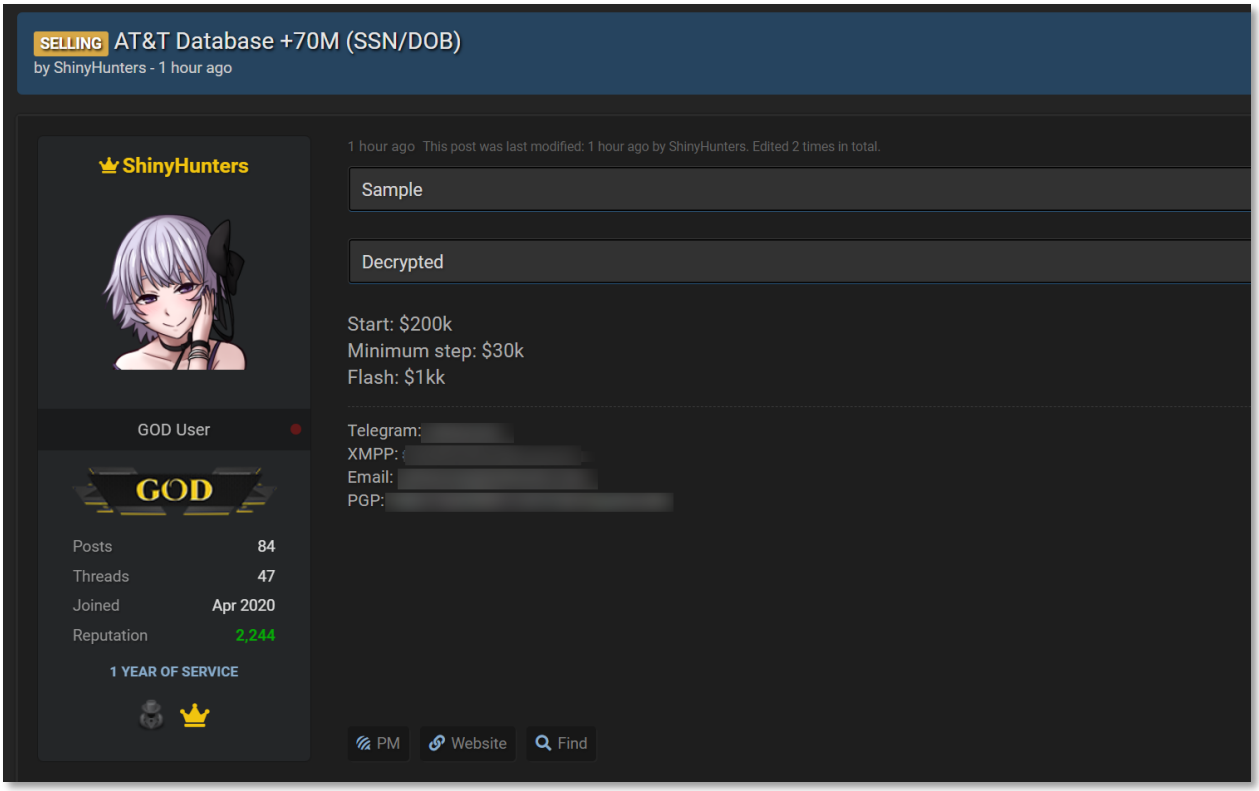
29. In connection with this data security priority, and "to protect network, data, mobility and cloud-based information resources in an era of large-scale, sophisticated attacks," AT&T purports to have "design[ed] and implement[ed] new security architecture based on the latest advances in virtualization, artificial intelligence, and networking."[12]

30. Despite AT&T's purported commitment to protecting the security of its customers' PII, however, AT&T failed to adequately secure the PII that it was entrusted, leading to the compromise of approximately 73 million current and former customers' PII.

[11] *Network & Data Security*, AT&T, https://sustainability.att.com/priority-topics/network-data-security (last visited Apr. 10, 2024).
[12] *Id.*

## B. The AT&T Data Breach.

31. AT&T first learned of the Data Breach in 2021, when a threat actor claimed to be selling a dataset containing the personal information of approximately 70 million customers. Specifically, in August of 2021, the threat actor began advertising a dataset on a hacking forum with a starting price of $200,000 and an immediate sale of $1,000,000:[13]




[13] Lawrence Abrams, *AT&T denies data breach after hacker auctions 70 million user database*, Bleeping Computer (Aug. 20, 2021), https://www.bleepingcomputer.com/news/security/atandt-denies-data-breach-after-hacker-auctions-70-million-user-database/.

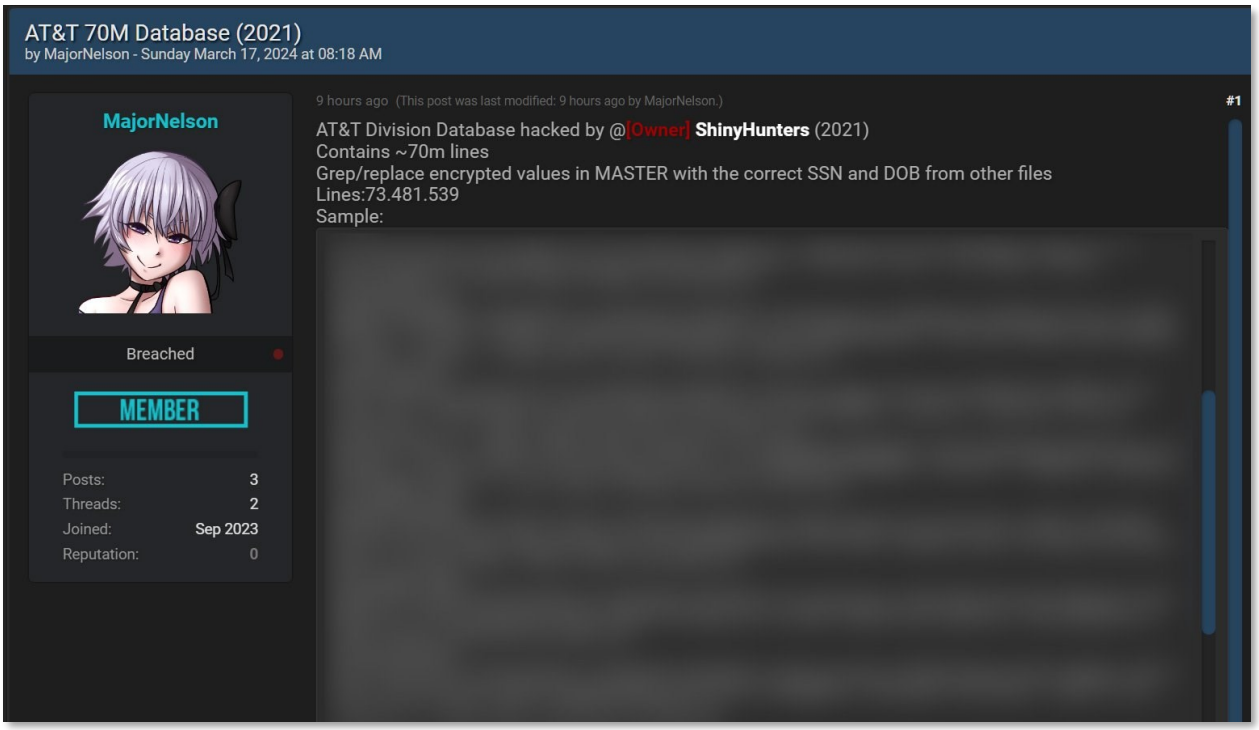
32. From the dataset samples shared at the time of auction by the threat actor, the database contained customer names, addresses, phone numbers, Social Security Numbers, and dates of birth. Security researchers were able to confirm that some of the dataset samples related to persons with AT&T accounts.[14]

33. At this time in 2021, however, AT&T denied that the compromised dataset was from AT&T, stating "[b]ased on our investigation today, the information that appeared in an internet chat room does not appear to have come from our systems."[15]

34. AT&T similarly refused to speculate on whether the dataset could have come from a third-party partner, stating: "[g]iven this information did not come from us, we can't speculate on where it came from or whether it is valid."[16]

35. Flashforward to nearly three years later, On March 17, 2024, a separate threat actor released a dataset on a hacking forum, claiming that it was the same AT&T dataset that was previously put up for sale in 2021:[17]

[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] *Abrams*, *supra* note 1.




36. Approximately two weeks later, on March 30, 2024, AT&T confirmed that the dataset released on to the dark web belonged to 7.6 million current AT&T customers and approximately 65.4 million former customers AT&T customers.[18]

37. On or about this same time, AT&T initiated as passcode reset for approximately 706 million current customers after it determined that customer passcodes were compromised during the Data Breach.[19]

38. On or about April 10, 2024, AT&T began notifying individuals impacted by the Data Breach. AT&T indicated that the information compromised during the Data Breach included a side variety of PII, including, *inter alia,* full

[18] *AT&T*, *supra* note 3.
[19] *Keeping your account secure*, AT&T, https://www.att.com/support/article/my-account/000101995?bypasscache=1 (last visited Apr. 10, 2024).

names, email addresses, mail addresses, phone numbers, Social Security Numbers, dates of birth, AT&T account numbers, and AT&T passcodes.[20]

**C. The Value of PII and Effects of Unauthorized Disclosure.**

39. AT&T understood the protected PII which it acquires is highly sensitive and of significant value to those who would use it for wrongful, nefarious purposes.

40. AT&T also knew that a breach of its computer systems, and exposure of the PII therein, would result in the increased risk of identity theft and fraud against the individuals whose PII was compromised.

41. Indeed, AT&T itself recognizes that it was a foreseeable target of cybercriminals, stating that "[c]yberattacks – including through the use of malware, computer viruses, distributed denial of services attacks, ransomware attacks, credential harvesting, social engineering and other means for obtaining unauthorized access to or disrupting the operation of [its] networks and systems and those of [its]suppliers, vendors and other service providers – could have a material adverse effect on [its] operations."[21]

---

[20] *Data Breach Notifications*, Office of the Maine Attorney General (Apr. 10, 2024), https://apps.web.maine.gov/online/aeviewer/ME/40/3778e1fc-2ed5-461d-9cc5-df15c07f687c.shtml (last accessed Apr. 10, 2024).

[21] *AT&T Form 10-K* (Dec. 31, 2023), https://otp.tools.investis.com/clients/us/atnt2/sec/sec-show.aspx?FilingId=17303532&Cik=0000732717&Type=PDF&hasPdf=1.

42. These risks are not theoretical, as numerous high-profile data breaches have occurred at telecommunications companies, including T-Mobile and Comcast d/b/a Xfinity.

43. PII is a valuable commodity to identity thieves. As the Federal Trade Commission ("FTC") recognizes, identity thieves can use this information to commit an array of crimes including identity theft, and medical and financial fraud.[22] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII and other protected financial information on multiple underground Internet websites, commonly referred to as the "dark web."

44. Criminals often trade stolen PII on the "cyber black market" for years following a breach. Cybercriminals can also post stolen PII on the internet, thereby making such information publicly available.

45. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the U.S. In 2021, there were

[22] *What To Know About Identity Theft*, Fed. Trade Comm'n Consumer Advice (Apr. 2021), https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last accessed Apr. 10, 2024).

4,145 publicly disclosed data breaches, exposing 22 billion records. The United States specifically saw a 10% increase in the total number of data breaches.[23]

46. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years. For instance, in 2017, 2.9 million people reported some form of identity fraud compared to 5.7 million people in 2021.[24]

47. The telecommunications sector is also a prime target for threat actors "due to their role in managing crucial communication networks that handle vast quantities of private and confidential information." As one news article explained: Telco is among the most-targeted sectors globally for cybercriminals, and it's not hard to see why. Sensitive user information is carried at a massive scale on telecom networks, and that naturally makes them an attractive target for malicious actors."[25]

---

[23] *Data Breach Report: 2021 Year End*, Risk Based Security (Feb. 4, 2022), https://www.riskbasedsecurity.com/2022/02/04/data-breach-report-2021-year-end/ (last accessed Apr. 10, 2024).

[24] *Insurance Information Institute, Facts + Statistics: Identity theft and cybercrime*, Insurance Information Institute, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019 (last accessed Apr. 10, 2024).

[25] Katy Allan, *The growing concerns in telecommunication cybersecurity*, Cyber Magazine (Oct. 30, 2023), https://cybermagazine.com/articles/the-growing-concerns-in-telecommunication-cybersecurity.

48. The ramifications of AT&T's failure to keep Plaintiffs' and Class Members' PII secure are long-lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

49. A data breach increases the risk of becoming a victim of identity theft. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice:

> A direct financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss.[26]

50. Even if stolen PII does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII about the individual, such as name, address, email

[26] Erika Harrell, Bureau of Just. Stat., U.S. Dep't of Just., NCJ 256085, *Victims of Identity Theft*, 2018 I (2020) https://bjs.ojp.gov/content/pub/pdf/vit18.pdf (last accessed Apr. 10, 2024).

address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

51. A poll of security executives predicted an increase in attacks over the next two years from "social engineering and ransomware" as nation-states and cybercriminals grow more sophisticated. Unfortunately, these preventable causes will largely come from "misconfigurations, human error, poor maintenance, and unknown assets."[27]

52. Due to high-profile data breaches at other companies, AT&T knew or should have known that the PII entrusted to it by its customers would be targeted by cybercriminals.

53. AT&T also knew or should have known the importance of safeguarding the PII with which it was entrusted and of the foreseeable consequences if that PII was breached. AT&T failed, however, to take adequate cybersecurity measures to prevent the Data Breach and release of its customers' PII from occurring.

## D. AT&T Failed to Comply with FTC Guidelines and Industry Best Practices.

54. AT&T is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or

[27] Chuck Brooks, *Alarming Cyber Statistics For Mid-Year 2022 That You Need to Know*, Forbes (June 3, 2022), https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=176bb6887864.

affecting commerce." FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

55. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[28]

56. The FTC recommends that companies verify that third-party service providers have implemented reasonable security measures.[29]

57. The FTC recommends that businesses:

a. Identify all connections to the computers where sensitive information is stored;

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks;

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business;

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an

[28] *Start with Security: A Guide for Business*, Fed. Trade Comm'n (June 2015) https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed Apr. 10, 2024).

[29] Erika Harrell, Bureau Of Just. Stat., U.S. Dep't of Just., NCJ 256085, *Victims of Identity Theft*, 2018 I (2020) https://bjs.ojp.gov/content/pub/pdf/vit18.pdf (last accessed Apr. 10, 2024).

internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine;

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks;

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet;

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically;

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day; and

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business's network, the transmission should be investigated to make sure it is authorized.

58. The FTC further recommends business take additional cybersecurity steps, which include:[30]

a. Conducting an inventory of all company devices that store sensitive data, and understanding what types of PII is stored on those devices;

b. Encrypting sensitive personal information stored on computer networks so that it is unreadable even if hackers are able to gain access to the information;

c. Crafting a data security plan that involves both physical security (*e.g.*, locking up physical files) and electronic security, and training employees regarding the data security plan.

d. Promptly disposing of PII that is no longer needed, and retaining sensitive data only as long as companies maintain a legitimate business need for the information; and

e. Developing a plan to handle a data breach or data security incident, if and when such an incident occurs.

59. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

[30] *Protecting Personal Information: A Guide for Business*, U.S. Federal Trade Comm'n (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed Apr. 10, 2024).

60. Upon information and belief, AT&T failed to properly implement one or more of the basic data security practices described above. AT&T's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII resulted in the unauthorized release of Plaintiffs' and Class Members' PII to threat actors. Further, AT&T's failure to implement basic data security practices constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

61. Similarly, the U.S. Government's National Institute of Standards and Technology ("NIST") provides a comprehensive cybersecurity framework that companies of any size can use to evaluate and improve their information security controls.[31]

62. NIST publications include substantive recommendations and procedural guidance pertaining to a broad set of cybersecurity topics including risk assessments, risk management strategies, access controls, training, data security controls, network monitoring, breach detection, and incident response.[32] Upon information and belief, AT&T failed to adhere to the NIST guidance.

[31] *See Framework for Improving Critical Infrastructure Cybersecurity*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (Apr. 16, 2018), Appendix A, Table 2, https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf.
[32] *Id.* at Table 2 pg. 26-43.

63. Upon information and belief, AT&T's failure to protect Plaintiffs' and Class Members' PII is a result of Defendants' failure to adopt reasonable safeguards as required by the FTC and NIST.

64. AT&T was, at all times, fully aware of its obligations to protect the PII of consumers because of its business model of collecting PII. AT&T was also aware of the significant repercussions that would result from its failure to do so.

## E. Plaintiffs' Experiences.

***Plaintiff Hasson***

65. Plaintiff Hasson is a current AT&T customer. In order to do business with AT&T, Plaintiff Hasson was required to entrust Defendants with his PII and, in return, reasonably expected that AT&T would safeguard his PII from unauthorized access.

66. Upon information and belief, Plaintiff Hasson's PII was compromised in the Data Breach. A search of Plaintiff Hasson's email address on the website "Have I been Pwned[33]," a website that allows individuals to check whether their PII has been compromised by data breaches, reveals that Plaintiff Hasson's PII was compromised in the Data Breach.

67. Plaintiff Hasson has suffered actual injury from having his PII exposed and/or released on the Dark Web as a result of the Data Breach, including:

[33] *See* https://haveibeenpwned.com/.

(1) required mitigation efforts, including needing to monitor his financial accounts to ensure his information is not used for identity theft and fraud; (b) damages to and diminution of the value of his PII, a form of intangible property that loses value when it falls into the hands of criminals who are using that information for fraud or publishing the information for sale on the dark web; (c) loss of privacy; and (d) continuous, imminent, and impending injury raising from increased risk of identity theft and fraud especially in light of the sensitivity of the PII compromised in the Data Breach.

***Plaintiff Chad Graddy***

68. Plaintiff Graddy was an AT&T customer. In order to do business with AT&T, Plaintiff Graddy was required to entrust Defendants with his PII and, in return, reasonably expected that AT&T would safeguard his PII from unauthorized access.

69. Plaintiff Graddy was required to provide his PII to Defendants as a condition of obtaining products and/or services from them. Upon information and belief, this PII included his name, date of birth, phone number, Social Security number, and other sensitive information.

70. At the time of the Data Breach, Defendants maintained Plaintiff's PII in their system.

71. Plaintiff Graddy received an email notice letter from AT&T that his personal information had been compromised. As a result, information in AT&T's possession including his full name, email address, mailing address, phone number, social security number, date of birth, AT&T account number, and passcode may all have been affected by the Data Breach.

72. Plaintiff is very careful about sharing his sensitive PII. Plaintiff stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff would not have entrusted his PII to Defendants had he known of Defendants' lax data security policies.

73. Upon information and belief, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties.

74. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach. Plaintiff has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to, work and/or recreation. This time has been lost forever and cannot be recaptured.

75. Plaintiff Graddy has suffered actual injury from having his PII exposed and/or released on the Dark Web as a result of the Data Breach, including:

(1) required mitigation efforts, including needing to monitor his financial accounts to ensure his information is not used for identity theft and fraud; (b) damages to and diminution of the value of his PII, a form of intangible property that loses value when it falls into the hands of criminals who are using that information for fraud or publishing the information for sale on the dark web; (c) loss of privacy; and (d) continuous, imminent, and impending injury raising from increased risk of identity theft and fraud especially in light of the sensitivity of the PII compromised in the Data Breach.

**F. Plaintiffs and Class Members Suffered Damages.**

76. The ramifications of AT&T's failure to keep user PII secure are long lasting and severe. Consumer victims of data breaches are more likely to become victims of identity fraud, occurring 65 percent of the time.[34]

77. In 2021 alone, identity theft victims in the United States had financial losses totaling $16.4 billion.[35]

[34] *What Are Your Odds of Getting Your Identity Stolen?*, IdentityForce (Apr. 15, 2021), https://www.identityforce.com/blog/identity-theft-odds-identity-theft-statistics.

[35] Erika Harrell & Alexandra Thompson, *Victims of Identity Theft, 2021*, U.S. Dept. Just., Bureau Just. Stats. (Oct. 2023), https://bjs.ojp.gov/document/vit21.pdf (last accessed Apr. 10, 2024).

78. In 2019, the United States Government Accountability Office ("GAO") released a report addressing the steps consumers can take after a data breach.[36] Its appendix of steps consumers should consider, in extremely simplified terms, continues for five pages. In addition to explaining specific options and how they can help, one column of the chart explains the limitations of the consumers' options. It is clear from the GAO's recommendations that the steps data breach victims (like Plaintiffs and Class Members) must take after a data breach, like Defendants', are both time-consuming and of only limited and short-term effectiveness.

79. The FTC, like the GAO, recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[37]

80. Ultimately, the time that victims spend monitoring and resolving identity theft issues takes an emotional toll. Approximately 80% of victims of

---

[36] Government Accountability Off., Data Breaches (Mar. 2019) https://www.gao.gov/assets/gao-19-230.pdf (last accessed Apr. 10, 2024).

[37] *See Identity Theft Victim Checklist,* Fed. Trade Comm'n, https://www.identitytheft.gov/Steps (last accessed Apr. 10, 2024).

identity theft experienced some type of emotional distress, and more than one-third of victims experienced moderate or severe emotional distress.[38]

81. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

82. As a result of AT&T's failure to prevent the Data Breach, Plaintiffs and Class Members have suffered and will continue to suffer injuries, including loss of time and productivity through efforts to ameliorate, mitigate, and deal with the future consequences of the Data Breach; theft of their highly valuable PII; the imminent and certainly impending injury flowing from fraud and identity theft posed by their PII being placed in the hands of criminals; damages to and diminution in value of their PII that was entrusted to Defendants with the understanding the Defendants would safeguard the PII against disclosure; and continued risk to Plaintiffs' and the Class Members' PII, which remains in the possession of Defendants and which is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect the PII with which it was entrusted.

[38] *Id.*

## CLASS ALLEGATIONS

83. Plaintiffs bring this case individually and, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of the class defined as:

> All individuals in the United States whose PII was compromised in the AT&T Data Breach which was announced on or about March 30, 2024 (the "Class").

84. Excluded from the Class are Defendants, their subsidiaries and affiliates, their officers, directors and members of their immediate families and any entity in which Defendants have a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

85. Plaintiffs reserve the right to modify or amend the definition of the proposed Class prior to moving for class certification.

86. **Numerosity.** The Class described above is so numerous that joinder of all individual members in one action would be impracticable. The disposition of the individual claims of the respective Class Members through this class action will benefit both the parties and this Court. The exact size of the Class and the identities of the individual members thereof are ascertainable through Defendants' records, including but not limited to, the files implicated in the Data Breach. Based upon public filings, the number of people impacted is approximately 73 million.

87. **Commonality.** This action involves questions of law and fact that are common to the Class Members. Such common questions include, but are not limited to:

a. Whether and to what extend Defendants had a duty to protect the PII of Plaintiffs and Class Members;

b. Whether Defendants were negligent in collecting and storing Plaintiffs' and Class Members' PII;

c. Whether Defendants had duties not to disclose the PII of Plaintiffs and Class Members to unauthorized third parties;

d. Whether Defendants took reasonable steps and measures to safeguard Plaintiffs' and Class Members' PII;

e. Whether Defendants failed to adequately safeguard the PII of Plaintiffs and Class Members;

f. Whether Defendants breached its duties to exercise reasonable care in handling Plaintiffs' and Class Members' PII;

g. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendants adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII had been compromised;

i. Whether Plaintiffs and Class Members are entitled to damages as a result of Defendants' wrongful conduct; and

j. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

88. **Typicality.** Plaintiffs' claims are typical of the claims of the Class Members. The claims of Plaintiffs and Class Members are based on the same legal theories and arise from the same failure by Defendants to safeguard their PII. Plaintiffs and Class Members entrusted Defendants with their PII, and it was subsequently released to an unauthorized third party.

89. **Adequacy of Representation.** Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the other Class Members Plaintiffs seek to represent; Plaintiffs have retained counsel competent and experienced in complex class action litigation; Plaintiffs intend to prosecute this action vigorously; and Plaintiffs' counsel has adequate financial means to vigorously pursue this action and ensure the interests of the Class will not be harmed. Furthermore, the interests of the Class Members will be fairly and adequately protected and represented by Plaintiffs and Plaintiffs' counsel.

90. **Superiority.** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class

treatment will create economies of time, effort, and expense and promote uniform decision-making.

91. **Predominance.** Common questions of law and fact predominate over any questions affecting only individual Class members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendants' liability and the fact of damages is common to Plaintiffs and each member of the Class. If Defendants breached their duty and released Plaintiffs' and Class Members' PII, then Plaintiffs and each Class member suffered damages by that conduct.

92. **Ascertainability:** Members of the Class are ascertainable. Class membership is defined using objective criteria, and Class Members may be readily identified through Defendants' books and records.

## FIRST CAUSE OF ACTION
## NEGLIGENCE
## (On Behalf of Plaintiffs and the Class)

93. Plaintiffs restate and reallege all proceeding allegations in paragraphs 1-92 above as if fully set forth herein.

94. Plaintiffs bring this claim individually and on behalf of the Class.

95. AT&T owed a duty under common law to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting,

and protecting their PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

96. Specifically, this duty included, among other things: (a) designing, maintaining, and testing AT&T's security systems to ensure that Plaintiffs' and Class Members' PII in AT&T's possession was adequately secured and protected; (b) implementing processes that would detect a breach of its security system in a timely manner; (c) timely acting upon warnings and alerts, including those generated by its own security systems, regarding intrusions to its networks; and (d) maintaining data security measures consistent with industry standards.

97. AT&T's duty to use reasonable care arose from several sources, including but not limited to those described below.

98. AT&T had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of Defendants. By collecting and storing valuable PII that is routinely targeted by criminals for unauthorized access, AT&T was obligated to act with reasonable care to protect against these foreseeable threats.

99. AT&T also owed a common law duty because its conduct created a foreseeable risk of harm to Plaintiffs and Class Members. Defendants' conduct included their failure to adequately restrict access to customer PII.

100. AT&T also knew or should have known of the inherent risk in collecting and storing massive amounts of PII, the importance of implementing adequate data security measures to protect that PII, and the frequency of cyberattacks such as the Data Breach in the telecommunications sector.

101. AT&T breached the duties owed to Plaintiffs and Class Members and thus was negligent. AT&T breached these duties by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust their information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow their own privacy policies provided to customers; (h) failing to adequately train and supervise employees and third party vendors with access or credentials to systems and databases containing sensitive PII and (i) failing to promptly disclose that Plaintiffs' and Class Members' PII had been or was reasonably believed to have been, stolen or compromised.

102. But for AT&T's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, their PII would not have been compromised.

103. As a direct and proximate result of AT&T's negligence, Plaintiffs and Class Members have suffered injuries including:

a. Theft of their PII;

b. Costs associated with requesting credit freezes;

c. Costs associated with the detection and prevention of identity theft;

d. Costs associated with purchasing credit monitoring and identity theft protection services;

e. Lowered credit scores resulting from credit inquiries following fraudulent activities;

f. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach;

g. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;

h. Damages to and diminution in value of their PII entrusted to AT&T with the mutual understanding that AT&T would safeguard Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others; and

i. Continued risk of exposure to hackers and thieves of their PII, which remains in AT&T's possession and is subject to further breaches so long as AT&T fails to undertake appropriate and adequate measures to protect Plaintiffs and Class Members.

104. As a direct and proximate result of AT&T's negligence, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

**SECOND CAUSE OF ACTION**
**NEGLIGENCE *PER SE***
**(On Behalf of Plaintiffs and the Class)**

105. Plaintiffs restate and reallege all proceeding factual allegations in paragraphs 1-92 above as if fully set forth herein.

106. Plaintiffs bring this claim individually and on behalf of the Class.

107. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as AT&T for failing to use reasonable measures to

protect PII. Various FTC publications and orders also form the basis of AT&T's duty.

108. AT&T violated Section 5 of the FTC Act by failing to use reasonable measures to protect customers' PII, not complying with the industry standards, and failing to timely notify Plaintiffs' and Class Members' data was compromised. AT&T's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of a data breach.

109. Plaintiffs and Class Members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

110. Moreover, the harm that has occurred is the type of harm that the FTC Act was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and Class Members.

111. AT&T's violation of Section 5 of the FTC Act constitutes negligence *per se*.

112. As a direct and proximate result of Defendants' negligence, Plaintiffs and Class Members have suffered injuries, including those identified in paragraphs 67 and 75 above.

113. As a direct and proximate result of AT&T's negligence, Plaintiffs and Class Members have been injured as described herein and above, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

## THIRD CAUSE OF ACTION
## BREACH OF IMPLIED CONTRACT
## (On Behalf of Plaintiffs and the Class)

114. Plaintiffs restate and reallege all preceding allegations in paragraphs 1-92 above as if fully set forth herein.

115. Plaintiffs bring this claim individually and on behalf of the Class.

116. AT&T required Plaintiffs and Class Members to provide their PII as a condition for using AT&T's services.

117. In doing so, Plaintiffs and Class Members entered into implied contracts with AT&T by which Defendants agreed to safeguard and protect such PII, keep such PII secure and confidential, and to timely and accurately notify Plaintiffs and Class Members if their PII had been breached, compromised, or stolen.

118. When entering into these implied contracts, Plaintiffs and Class Members reasonably believed and expected that AT&T's data security practices complied with its statutory and common law duties to adequately protect Plaintiffs' and Class Members' PII and to timely notify them of a data breach.

119. Indeed, implicit in these exchanges was a promise by Defendants to ensure the PII of Plaintiffs and Class Members in its possession would be used to provide the agreed-upon services and that AT&T would take adequate measures to protect Plaintiffs' and Class Members' PII and timely notify them in the event of a data breach.

120. It is clear by these exchanges that the parties intended to enter into implied agreements supported by mutual assent. Plaintiffs and Class Members would not have disclosed their PII to Defendants but for the prospect of Defendants' promise of services. Conversely, AT&T presumably would not have taken Plaintiffs' and Class Members' PII if it did not intend to provide Plaintiffs and Class Members services.

121. Plaintiffs and Class Members would not have provided their PII to AT&T had they known that Defendants would not safeguard their PII as promised or provide timely notice of a data breach.

122. Plaintiffs and Class Members fully performed their obligations under their implied contracts with AT&T.

123. AT&T breached its implied contracts with Plaintiffs and Class Members by failing to safeguard Plaintiffs' and Class Members' PII and by failing to provide them with timely and accurate notice of the Data Breach.

124. As a direct and proximate result of AT&T's breach of implied contract, Plaintiffs and Class Members have suffered injuries, including those identified in paragraphs 67 and 75 above.

125. As a direct and proximate result of AT&T's breach of contract, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

## FOURTH CAUSE OF ACTION
## UNJUST ENRICHMENT
## (On Behalf of Plaintiffs and the Class)

126. Plaintiffs restate and reallege all preceding allegations in paragraphs 1-92 above as if fully set forth herein.

127. Plaintiffs bring this claim individually and on behalf of the Class.

128. Plaintiffs bring this claim in the alternative to their breach of implied contract claim.

129. By engaging in the conduct described in this Complaint, AT&T has knowingly obtained and derived benefits from Plaintiffs and Class Members at Plaintiffs' and Class Members' expense, namely the profits gained from payment in exchange for the use of AT&T's services, such that it would be inequitable and unjust for Defendants to retain.

130. By engaging in the acts and failures to act described in this Complaint, AT&T has been knowingly enriched by the savings in costs that should have been

reasonably expensed to protect the PII of Plaintiffs and the Class. Defendants knew or should that known that theft of consumer PII could happen, yet it failed to take reasonable steps to pay for the level of security required to have prevented the theft of its consumers' PII.

131. AT&T's failure to direct profits derived from Plaintiffs' and Class Members' payments for services toward safeguarding Plaintiffs' and Class Members' PII constitutes the inequitable retention of a benefit without payment for its value.

132. AT&T will be unjustly enriched if it is permitted to retain the benefits derived after the theft of Plaintiffs' and Class Members' PII.

133. Plaintiffs and Class Members have no adequate remedy at law. As a direct and proximate result of AT&T's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

134. AT&T should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them.

## FIFTH CAUSE OF ACTION
## DECLARATORY JUDGMENT
## (On Behalf of Plaintiffs and the Class)

135. Plaintiffs restate and reallege all proceeding factual allegations in paragraphs 1-92 above as if fully set forth herein.

136. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal laws and regulations described herein.

137. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and Class Members' PII and whether AT&T is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their PII. Plaintiffs allege that Defendants' data security measures remain inadequate. Furthermore, Plaintiffs and Class Members continue to suffer injury as a result of the compromise of their PII and remain at imminent risk that further compromises of their PII will occur in the future.

138. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. AT&T owes a legal duty to secure consumers' PII and to timely notify consumers of a data breach under the common law and Section 5 of the FTC Act; and

b. AT&T continues to breach this legal duty by failing to employ reasonable data security measures to safeguard Plaintiffs' and Class Members' PII.

139. This Court also should issue corresponding prospective injunctive relief requiring AT&T to employ adequate security protocols consistent with law and industry standards to protect consumers' PII.

140. If an injunction is not issued, Plaintiffs and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at AT&T. The risk of another such breach is real, immediate, and substantial. If another breach at AT&T occurs, Plaintiffs and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

141. The hardship to Plaintiffs and Class Members if an injunction is not issued exceeds the hardship to AT&T if an injunction is issued. Plaintiffs and Class Members will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to AT&T of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and AT&T has a pre-existing legal obligation to employ such measures.

142. Issuance of the requested injunction will not disserve the public interest. On the contrary, such an injunction would benefit the public by preventing another data breach at AT&T, thus eliminating the additional injuries that would result to

Plaintiffs and consumers whose confidential information would be further compromised.

## PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated, pray for relief as follows:

1. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiffs as representatives of the Class and Plaintiffs' attorneys as Class Counsel to represent the Class;
2. For an order finding in favor of Plaintiffs and the Class on all counts asserted herein;
3. For damages in an amount to be determined by the trier of fact;
4. For an order of restitution and all other forms of equitable monetary relief;
5. Declaratory and injunctive relief as described herein;
6. Awarding Plaintiffs' reasonable attorneys' fees, costs, and expenses pursuant to O.C.G.A. Section 13-6-11 and as otherwise allowed by law;
7. Awarding pre- and post-judgment interest on any amounts awarded; and,
8. Awarding such other and further relief as may be just and proper.

## JURY TRIAL DEMANDED

A jury trial is demanded on all claims so triable.

Dated: April 15, 2024

Respectfully submitted,

*/s/ MaryBeth V. Gibson*
MaryBeth V. Gibson
Georgia Bar No. 725843
**GIBSON CONSUMER LAW GROUP, LLC**
4729 Roswell Road
Suite 208-108
Atlanta, GA 30342
Telephone: (678) 642-2503
marybeth@gibsonconsumerlawgroup.com

Gary F. Lynch (*pro hac vice* forthcoming)
**LYNCH CARPENTER LLP**
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
Telephone: (412) 322-9243
gary@lcllp.com

Jennifer M. French (*pro hac vice* forthcoming)
**LYNCH CARPENTER, LLP**
1234 Camino Del Mar
Del Mar, CA 92014
Telephone: (619) 762-1900
jennf@lcllp.com

*Attorneys for Plaintiffs and the Class*